

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Scott Labor, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with Homeland Security, Immigration and Customs Enforcement; Homeland Security Investigations (HSI). I am currently assigned to the Office of the Special Agent in Charge, Boston, Massachusetts, and have been employed in that capacity since June 2005. Since June 2013, I have been assigned to HSI Derby Line, Vermont. I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and work relating to conducting these types of investigations. I have had discussions with other law enforcement officers, including Vermont Office of Attorney General Detective Matthew Raymond, about how people use electronic media to commit crimes and the law enforcement techniques that can be utilized to investigate and disrupt such activity. I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. I make this affidavit in support of an application for a search warrant for information associated with the account bearing usernames: “ZaneSalvatore#2521,” and “Katsuki Bakugo” (the “Target Account”), such information being stored at premises controlled

by Discord Inc. (“Discord”), a proprietary freeware VOIP (Voice Over Internet Protocol) application and digital distribution platform designed for video gaming communities that specializes in text, image, video and audio communication between users in a chat channel, headquartered at 444 De Haro St, Suite 200, San Francisco, CA 94107.

3. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Discord to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

4. Based on my training and experience and the facts as set forth in this affidavit, I believe that there is probable cause to believe that offenses of (i) Receipt and Distribution of Child Pornography, in violation of 18 U.S.C. § 2252(a)(2); and (ii) Possession of and Access with Intent to View Child Pornography, in violation of 18 U.S.C. § 2252(a)(4), have been committed by the user of the Target Account. I also believe that there is probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, or fruits of the crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that—has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

6. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in Attachment A of this Affidavit, including records related to the Target Account for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4), which items are more specifically described in Attachment B of this Affidavit.

7. The statements in this Affidavit are based in part on information provided to me by other law enforcement officers, and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of child pornography offenses will be found in the Target Account.

STATUTORY AUTHORITY

8. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

DEFINITIONS

9. The following definitions apply to this Affidavit and Attachment B:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that

creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. “Geolocated,” as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A “hash value” is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

k. “Internet Protocol” (IP) Addresses: An IP address is assigned to every device participating in a computer network that uses the internet protocol for communication. There are two commonly used types of IP addresses called IPv4 and IPv6.

(1) IPv4, or IP version 4, is a 32-bit numeric address that consists of a series of four numbers, each ranging between 0 and 255, that are separated by dots. An example of an IPv4 address is 123.111.123.111.

(2) IPv6, or IP version 6, is a 128-bit hexadecimal address that consists of a series of eight values separated by colons. Hexadecimal values consist of a series of numbers between 0 and 9 and letters between A and F. An example of an IPv6 address is: 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

(3) When a device accesses the internet, it uses a source IP address and a destination IP address to communicate. The source IP address acts as the address from where the device, such as a computer, accesses the internet. The destination IP address acts as the address to where a user wishes to go, such as a website.

(4) The use of IP addresses is what allows traffic on the internet to be properly directed from the correct source to the correct destination.

(5) Most internet service providers control a range of IP addresses which are assigned to their subscribers to allow them to communicate on the internet with their

devices. They can be assigned statically so the IP address never changes, or they can be assigned dynamically where a user is assigned an available IP address within their internet service provider's range of IP addresses at the time they access the internet.

(6) It is possible to determine if a particular IP address is likely located within the State of Vermont by using IP geographic mapping services, which are publicly available and also used for marketing and fraud detection.

(7) It is also possible to determine the internet service provider providing the IP address by conducting a search of a Regional Internet Registry (RIR). There are a total of five RIRs. RIRs provide, amongst other things, IP address space allocation. This means that they allocate and distribute IP address amongst internet service providers located in their respective service region. The American Registry for Internet Numbers (ARIN) was established in 1997 as a RIR incorporated in Virginia. ARIN services Canada, many Caribbean and North Atlantic islands as well as the United States.

(8) The internet service provider can provide the subscriber information associated with an IP address used at a specific date and time. This subscriber information will provide the physical location of the access as well as the name, address, and other contact information for the person associated with the internet account that was using the IP address on the date and time in question.

1. "Carrier Grade Network Address Translation" (CGN): CGN technologies are used by some internet service providers to share one single IP address among multiple subscribers at the same time.

(1) On the internet, every connected device needs an IP address. However, the number of IP addresses (IPv4) is limited and insufficient to meet the exploding demand for new addresses for connected devices like smart phones. The new version of IP address (IPv6) which provides an unlimited number of IP addresses is available but the transition from IPv4 to IPv6 requires Internet service providers and internet content providers (websites, social media, webmail services, etc.) to update software and hardware. To address this problem, Internet service providers adopted CGN technologies which allow sharing of IPv4 addresses with multiple internet users (several thousands). This was supposed to be a temporary solution until the transition to IPv6 was completed but for some operators it has become a substitute for the IPv6 transition.

(2) One-way CGN technology is able to utilize the same IPv4 address for multiple users is to assign each user a unique source port number when the IPv4 address is assigned.

(3) If a user was assigned the port number of 450 utilizing an IP address of 123.111.123.111, it would commonly be represented as 123.111.123.111:450. The user would be the only one assigned the IP address and that specific port number at that time.

(4) An ISP utilizing this CGN technology would need to be provided the IP address along with the source port number along with the date and time of use to be able to provide the unique subscriber information for the user.

m. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

n. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

p. “Mobile application” or “chat application,” as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

q. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

r. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

s. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

t. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

u. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

v. “PhotoDNA” is a technology developed by Microsoft and improved by Dartmouth College that computes hash values of images, video and audio files to identify alike images. PhotoDNA is primarily used in the prevention of child pornography and works by computing a unique hash that represents the image. This hash is computed such that it is resistant to alterations in the image, including resizing and minor color alterations. It works by converting the image to black and white, re-sizing it, breaking it into a grid, and looking at intensity gradients or edges.

w. A GIF (Graphical Interchange Format) is an image format that supports both animated and static images. In short, GIFs are a series of images that will loop continuously and doesn't require anyone to press play and can appear to play like a video file.

DISCORD

10. Discord is a voice, video, media, and text (chat) communication service/platform in which users can communicate in private chats, ranging from 1-10 users, or as part of a larger group/community called servers. Servers are also broken down into subcategories, or channels. Discord maintains these media, and text (chat) communications, whether they occurred on a server or in private chats. Discord asks each of their subscribers to provide certain identifying information when registering for an account. This information can include, but is not limited to: a username, subscriber's full name, date of birth, physical address, telephone numbers, other identifiers, and/or e-mail addresses (which Discord can indicate if this email address has been verified or not). Information provided to and maintained by Discord by paying subscribers can include a means and source of payment (creditor bank account number).

11. Discord assigns a unique 18-digit User ID after an account is created. Discord and other providers of similar services, retain certain transactional information about the creation and use of each account on their systems. This information can include, but is not limited to: the date and time at which the account was created, the length of service, records of log-in (i.e., session) times and durations, friends list, the status of the account (including whether the account

is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account.

12. Discord also has records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses with logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account. In some cases, an account user will communicate directly with a provider, in this case, Discord, about issues relating to their account, such as technical problems, billing inquiries, and/or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user because of the communications.

13. Information related to the Target Account is stored at premises owned, maintained, controlled, or operated by Discord Inc., headquartered at 444 De Haro St, Suite 200, San Francisco, CA 94107.

PROBABLE CAUSE

14. In March 2023, HSI Derby Line, VT, was contacted by M.C. M.C. stated that she discovered that her 12-year-old daughter (hereinafter “MV1”) had been communicating with an adult male over Discord and that these chat communications were sexual in nature. M.C. stated that MV1 sent sexually explicit images of her vagina and breasts to the adult male via Discord.

15. On March 06, 2023, your affiant met with and interviewed M.C. M.C. stated that MV1 had recently been spending a lot of time in her bedroom, M.C. stated that this was not normal for her daughter. M.C. stated that she recently went through her daughter’s Apple Iphone and noticed that MV1 was communicating with an adult male via Discord. M.C. stated that

MV1 used Discord account “devilfox177” and the adult male used “ZaneSalvatore#2521”. M.C. consented to a search of MV’s Apple Iphone and signed a HSI consent to search form. M.C. further gave consent for HSI Derby Line to assume the online presence of MV1’s Discord account and signed an HSI consent to assume online presence form.

16. On March 06, 2023, your affiant reviewed the contents of MV1’s Discord account. Several of the chats with username: “ZaneSalvatore#2521” were sexually explicit. During one such chat, on March 01, 2023, “ZaneSalvatore#2521” instructed MV1 to send him a regular image and one of her spreading her “pussy”, stating: “hmm a regular one and one of you spreading your pussy not your legs but using two fingers to spread your pussy apart.” MV1 complied and sent “ZaneSalvatore#2521” two images, one image depicted herself laying on a bed naked from the waist down, the second image depicted her laying down on a bed with her legs spread using two fingers to spread her vagina, the focus of the image is of her vagina. On March 01, 2023, “ZaneSalvatore#2521” further instructed MV1 to send images of her “boobs”, stating: “hmm just a picture of your boobs and then one of you grabbing your boob.” MV1 complied and sent “ZaneSalvatore#2521” two images, the first image depicted MV1 standing up with her shirt pulled up exposing her breasts, the focus of the image is on her breasts, the second image depicts MV1 standing up with her shirt pulled up exposing her breasts, MV1’s hand is holding one of her breasts.

17. On March 08, 2023, Discord responded to a HSI summons requesting information for the target account and provided the following information:

- User ID: 1013225501982216223
- Username: ZaneSalvatore#2521
- Email: proherodynamite12@gmail.com
- Registration Time UTC: 2022/08/27 23:16:24
- Last Seen Time UTC: 2023-03-08 17:41:25
- Last seen IP: 67.219.80.176

18. On March 16, 2023, HSI Forensic Interviewer Emily Rivera-Nunez conducted a forensic interview with MV1. During the interview MV1 confirmed that she communicated via chats and video/live stream with "ZaneSalvatore#2521." MV1 stated that she told "ZaneSalvatore#2521" that she was 13 years old. MV1 stated that "Zane Salvatore#2521" told her he was 18. MV1 further stated she sent sexually explicit images via Discord to "ZaneSalvatore#2521" after he asked for them.

19. On April 06, 2023, I further reviewed the contents of MV1's Discord account. I was unable to locate the messages between "Zane Salvatore#2521" and MV1 that I had reviewed on March 06, 2023. However, I did see messages between MV1 and username "Katsuki Bakugo" that I had not seen previously. I opened the chat and noticed that the messages were in fact the same messages that I previously reviewed between "Zane Salvatore#2521," and MV1. I believe that the user of "Zane Salvatore#2521" has changed his username to: "Katsuki Bakugo."

REQUEST

20. I request permission to search for and seize Discord Inc. records related to Discord account bearing usernames "ZaneSalvatore#2521" and "Katsuki Bakugo." The Discord records will be searched for evidence of the sexual exploitation of children in violation 18 U.S.C. § 2252. Because in my training and experience, I have learned that many people who use social media accounts to trade and receive child pornography retain such materials for long periods of time and because information within the account may help identify the account user, I am seeking records from August 27, 2022, thru April 12, 2023.

21. In these cases, it is also important to search the account for user attribution to prove ownership of the account, user(s) of the account and, most importantly, who was in control of the account during the commission of the crime. To accomplish this one must look

for user attribution over a significant period of time, not just the hours surrounding a particular event. User attribution can be found in all types of files, exif data, and metadata.

22. The following is information available from Discord regarding user attribution.

a. Any and all subscriber information such as: name, address, telephone number, date of birth, date account created, account status, payment information, associated email addresses, any other accounts that share the same SMS or secondary email address as the specified account, as well as any other accounts that use the target email address as a secondary email, mailing address, phone number.

b. Records regarding any Android device information, including IMEI/MEID, make and model, serial number, date and IP of last access to Discord, and a list of all accounts that have ever been active on the device.

c. Communications between Discord and any person regarding the account, including contacts with support services and records of actions taken.

d. The contents of all communications stored in Discord. This can include any read, drafted, sent, or saved communications (inbox / outbox, trash/deleted, saved, and drafts folders) – both read and unread – including IP access logs relevant to this account and any saved member internet protocol addresses and connection logs.

23. Discord was sent preservation request under 18 U.S.C. § 2703(f) to preserve “all stored communications, records, and other evidence” regarding the Target Account.

CONCLUSION

24. Based on the foregoing, I believe that there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

25. Based on the foregoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Discord who will then compile the requested records at a

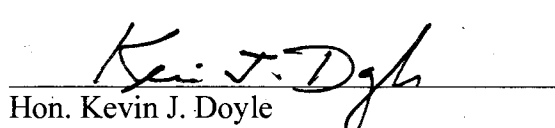
time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

26. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the Target Account. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.



Scott Labor
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this th12 day of April 2023.



Hon. Kevin J. Doyle
United States Magistrate Judge